National Archives and Records Administration

NARA 804
July 18, 2005

SUBJECT: Information Technology (IT) Systems Security

TO: Office Heads, Staff Directors, ISOO, NHPRC, OIG

Purpose of this transmittal memo. This transmits a revised policy directive, NARA 804, Information Technology (IT) Systems Security. NARA continues to review the supplements to the directive to update and expand this information as necessary to meet NARA's IT systems security needs.

Why has this directive been revised? We have revised NARA 804 to reflect current practices and updated authorities.

Whom can I contact if I have questions about this directive? Contact Leo Scanlon or Rob Neal (NHI) in room 4400, AII; on 301-837-0752, or 301-837-1980; by fax on 301-837-3213; or by e-mail.

Canceled directives. This directive cancels previous versions of NARA 804. The supplements to NARA 804 are unaffected by this revised directive.

ALLEN WEINSTEIN
Archivist of the United States

National Archives and Records Administration

NARA 804
July 18, 2005

SUBJECT: Information Technology (IT) Systems Security

804.1 What is the purpose of this directive?

a. This directive establishes policy and guidance for securing all electronic information collected or maintained by or on behalf of the National Archives and Records Administration (NARA) and the information systems used or operated by or on behalf of NARA. This directive also defines the role of information security in the context of an overall enterprise architecture.

b. This directive also delineates the security management program structure, assigns responsibilities, and creates the foundation necessary to measure progress and compliance. The specific standards and procedures for implementation of NARA IT security policy are contained in the supplements to this directive**.**

804.2 Authorities
44 U.S.C. 2108; 5 U.S.C. 552, as amended; 5 U.S.C. 552a, as amended, E.O. 12958; 40 U.S.C. 1401 through 1503, Information Technology Management Reform Act (Clinger-Cohen Act of 1996); Federal Information Security Management Act (FISMA) of 2002 (PL 107-347). FISMA reinforces past legislation (the Computer Security Act of 1987, the Clinger-Cohen Act, and the Paperwork Reduction Act) requiring each agency to implement an IT systems security program..

804.3 What additional documents provide guidance for the security of NARA's IT systems?

a. The ***NARA IT Security Architecture (SA)*** **section of NARA's Enterprise Architecture (EA)**, available on NARA@work under Information Technology, prescribes a level of security for NARA systems and provides guidance to system owners, Information System Security Officers (ISSO), and to all those who are responsible for the design, development, implementation, maintenance, and security of an information system. The security architecture also prescribes the technological framework for NARA's security program and identifies the controls that shape security policy.

b. **The IT security supplements** to this directive provide specific detailed implementation guidance for NARA systems that is to be used by ISSOs, system administrators, and all persons responsible for implementing and administrating NARA standard security settings on information systems.

c. **NARA 805, Systems Development Lifecycle (SDLC),** provides guidance and requirements, including those related to security, for project teams who are planning and implementing the development, evaluation, and maintenance of NARA's IT systems.

d. **Interim Guidance 202-01, NARA Information Security Program,** provides guidance for those persons responsible for the protection and control of classified national security information and sensitive unclassified information.

804.4 What are some external directives that affect NARA's information technology systems security program?

Federal agencies, including NARA, are subject to Federal security requirements, including legislation (cited in par. 804.2), Presidential Directives, mandates of oversight agencies, and standards, including:

a. Presidential Directives

(1) **Presidential Decision Directive 67** (**PDD-67)**, Enduring Constitutional Government and *Continuity of Government Operations,* 1998.

(2) **Homeland Security Presidential Directive-7, (HSPD-7),** *Critical Infrastructure Identification, Prioritization, and Protection, 2003.* Requires each agency to develop a plan to protect its critical information infrastructure.

(3) **HSPD-12,** *Policy for a Common Identification Standard for Federal Employees and Contractors, 2004*.

b. OMB Issuances

(1) **OMB A-130.** Office of Management and Budget Circular A-130, Appendix III – *Security of Federal Automated Information Resources.* Guidance to all Federal agencies about the development and implementation of IT systems security programs.

(2) **OMB Memos.** Office of Management and Budget Memos, especially M03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, and M05-04, Policies for Federal Agency Public Websites.

c. Standards

(1) **FIPS.** The National Institute of Standards (NIST) Federal Information Processing Standards.

(2) **NIST SP 800 Series**. National Institute of Standards (NIST) Special Publications as mandated by FIPS, especially NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems", December 1998. Provides direction to all Federal agencies for preparing IT systems security plans.

d. Other

(1) **Committee on National Security Systems (CNSS) Issuances.** CNSS issuances detail policy, direction, operational procedures, and guidance for the security of national security systems.

(2) **DCID 6/3.** Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information Within Information Systems.*

804.5 To which systems does this directive apply?
This directive applies to all information systems used or operated by, or on behalf of, NARA.

804.6 To whom does this directive apply?
This policy applies to all NARA employees, contractors, Foundation staff and Foundation-funded employees, interns, volunteers, detailees, and others who have access to NARANET and are authorized to use NARA information systems.

804.7 Definitions
All IT terms used in conjunction with this policy, the IT Security program, or the NARA IT Security Architecture are defined in the *NARA Enterprise Architecture Glossary of Terms and Acronyms*, available on NARA@work under Information Technology.

804.8 Responsibilities

a. **Chief Information Officer (CIO)** ensures that development and implementation of the NARA IT Security program and NARA IT security architecture conform to all NARA and other Federal standards, policies, and guidelines. The Assistant Archivist for Human Resources and Information Services (NH) is NARA's CIO.

b. **Chief Information Security Officer (CISO) i**s responsible for the implementation of this directive and its policies. Manages the NARA IT Security Program, with the mission and resources to ensure agency compliance with FISMA and other government-wide IT security policies through the development, implementation, and management of NARA IT systems. Director, IT Security Programs (NHI) serves as NARA's CISO.

c. **Chief Technology Officer (CTO)** develops, implements, and manages the NARA IT security architecture as part of the NARA Enterprise Architecture (EA).

d. **IT Security Staff (NHI)** plans and manages the IT Security program in conformance with the IT Security Architecture. The staff assists in the development of the security architecture, assures the appropriate integration of security controls as part of the systems engineering process, and provides guidance and assistance to systems owners on matters of IT security.

e. **System Developers** are responsible for developing, documenting, and testing their systems, hardware, firmware, software, and operations in conformance to the IT Security Architecture as directed by the IT Security program.

f. **System Administrators** are responsible for implementing, operating, and monitoring all NARA systems in conformance to the IT Security Architecture as directed by the IT Security program.

g. **Office Heads, Presidential Library Directors, and Regional Administrators** are responsible for ensuring compliance with this policy within their respective offices.

h. **System Owners** are the officials who have primary responsibility for determining that an IT system meets the business requirements of NARA, and who have responsibility for the procurement, development, and operation and maintenance of that system. System owners also evaluate the cost and benefits of system features, including the security costs of mitigating any vulnerabilities associated with the system. The System Owner also identifies or designates responsibility for two system functions: Data Owner (sometimes referred to as Information Owner) and the ISSO.

i. **Data Owner (or Information Owner)** has statutory or operational authority for information used by a system, and has responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

j. **Information Systems Security Officer (ISSO)** has the responsibility to ensure that the appropriate operational security posture is maintained for an information system or program. The ISSO assists in determining the security controls that are appropriate for the system, and provides information necessary to complete regular assessments of the system and the Plan of Action and Milestones (POA&M), which tracks response to internal and external audit findings.

k. **Managers and supervisors** throughout NARA ensure that their staff and authorized personnel are aware of and comply with this policy.

l. **System Users** include all NARA employees, contractors, Foundation Staff and Foundation-funded employees, interns, volunteers, detailees, and others who have access to NARANET and are authorized to use NARA information systems. Users are responsible for :

(1) Adhering to the terms of the NARA acceptable use policy, NARA 802, Appropriate Use of NARA Office Equipment;

(2) Completing the annual security and awareness training provided by NARA; and

(3) Ensuring that passwords and other access credentials are not shared or made available to unauthorized persons.

804.9 Why does NARA have an IT Security Program?

NARA develops, documents, and implements an IT security program to provide oversight, monitoring, compliance assessments, and program management for the electronic information and information systems that support the operation and assets of NARA, including those

provided by or managed by another agency, contractor, or other source. These security activities comply with applicable Federal statutes, and must align with the standards specified in the NARA IT security architecture.

804.10 What are the objectives of the NARA IT Security Program?
The security program is the means by which NARA plans for security, ensures that the appropriate officials are assigned security responsibility, provides appropriate training awareness to system users and authorizes system processing before operations and periodically afterward. The components of NARA's IT Security program:

a. Implement information security standards that meet the requirements promulgated under 40 U.S.C. 11331.

b. Implement information security standards and guidelines for NARA IT systems issued in accordance with law and as directed by the President,

c. Ensure that information security management processes are integrated with agency strategic and operational planning processes, and

d. Ensure that NARA provides for the security of information and information systems that support the operations and assets under their control.

e. Provide information security protections commensurate with the risks and magnitude of harm that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of:

(1) Information collected or maintained by, or on behalf of, NARA; and

(2) Information systems used or operated by, or on behalf of, NARA.

f. Implement the NARA Training and Awareness program.

804.11 How is the IT Security Program integrated with the Systems Development Lifecycle (SDLC), NARA 805?
NARA 805, Systems Development Lifecycle, specifies the creation of a system security plan as an integrated component of system development and acquisition. The NARA IT security program assists system owners in meeting their obligations in identifying, processing, planning, and managing risks that could impact on NARA operations, NARA assets, or individuals through four security processes.

a. **Certification, Accreditation (C&A), and Security Assessments** determine the extent to which the security controls in each information system is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The C&A process:

(1) Addresses specific existing or planned actions to correct deficiencies in

the security controls and to reduce or eliminate known vulnerabilities in the information system; and

(2) Determines whether the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals.

b. **Risk Management** is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management enables NARA to accomplish its mission by:

(1) Better securing the IT systems that store, process, or transmit NARA information;

(2) Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and

(3) Assisting the CIO in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk assessments.

c. **Continuous Monitoring** activities involve ongoing assessment of IT security controls on a continual basis, as opposed to performing a point-in-time assessment. Continuous monitoring is achieved through the use of various tools that include, but are not limited to, intrusion detection systems, vulnerability scanners, log servers, and security information management tools.

d. The **NARA Training and Awareness program** ensures that all people involved in using and managing IT systems understand their roles and responsibilities related to NARA's mission, understand the NARA's IT security policy, procedures, and practices, and have adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

804.12 How does the IT security program facilitate risk management?

a. The NARA IT security program ensures that security measures are adequate, or appropriate for the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. The certification and accreditation process is the means by which the security program helps responsible agency officials to understand the risks and other factors that could negatively impact their mission goals. It also allows them to make informed judgments and investments that appropriately keep risks at acceptable levels.

b. The assessment of security risk and the development of system security plans are two important activities in NARA's information security program that directly support the security certification and accreditation process, and are required by FISMA and OMB Circular A-130.

(1) The risk assessment influences the development of the security controls for particular information systems and generate much of the information needed for the associated system security plans.

(2) System security plans provide an overview of the information security requirements and describe the security controls in place or planned for meeting those requirements.

c. Risk management allows System Owners to balance the operational and economic costs of protective measures and increase mission capability by protecting the IT systems and data that support NARA's mission. The principal goal of NARA's risk management process is to protect the *organization and its ability to perform its mission*, not just its IT assets.

804.13 How is this directive related to the NARA Enterprise Architecture?
The *NARA IT Security Architecture* section of NARA's Enterprise Architecture (EA) establishes a framework by which a level of security for all NARA information systems is prescribed through a comprehensive and authoritative set of documentation that is appropriate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems. The documentation:

a. Categorizes and describes the major elements that comprise and affect NARA's IT operating environment from an IT security perspective;

b. Defines NARA's IT security goals, principles and policies;

c. Defines NARA's IT risk profile;

d. Categorizes the security needs of NARA's information assets;

e. Identifies and specifies NARA's requirements for IT security management, IT security processes and IT security technologies across the agency; and

f. Provides architectural designs and engineering specifications for implementing and integrating IT security mechanisms.

804.14 Why are the supplements to this directive important?
Specific standards and procedures for implementation of NARA IT security policy are contained in the supplements, in the form of handbooks, associated with this directive. The standards and procedures are subdivided into three major control areas: management, operational, and technical.

a. **Management Controls.** This supplement describes the management of the IT security system and the management of system risk normally addressed by IT management.

b. **Operational Controls.** This supplement addresses security methods focusing on the mechanisms primarily implemented and executed by people. These controls are established

to improve the security of a group, a particular system, or a group of systems. These controls require technical or specialized expertise and rely on management and technical controls.

c. **Technical Controls**. This supplement focuses on security controls that a computer system executes. These controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

d. The current version of the supplements can be found on NARA@work.

804.15 How are records created by this directive maintained under the NARA records schedule?

Records produced or maintained in the fulfillment of this directive are filed in accordance with the disposition instructions in NARA Records Schedule, item 830, Files Related to Maintaining the Security of Systems and Data.